SOLUTION BRIEF

ADVANCED THREAT PREVENTION WITH A10 NETWORKS AND OPSWAT

DISCOVER AND BLOCK ADVANCED ENCRYPTED THREATS HIDDEN IN SSL/TLS TRAFFIC WITH THE THUNDER SSLi AND METADEFENDER JOINT SOLUTION

A10 Networks and OPSWAT offer a comprehensive network security solution that discovers and blocks malicious attacks hidden in encrypted traffic. A10 Thunder® SSLi® (SSL Insight®) decrypts SSL-encrypted traffic across all TCP ports, enabling the OPSWAT MetaDefender ICAP Server to apply multi-scanning, data sanitization with content disarm & reconstruction (CDR), and data loss prevention (DLP) to the clear-text traffic.

THE CHALLENGE

ENCRYPTED CYBERATTACKS, MALWARE AND DATA EXFILTRATION CAN PASS THROUGH YOUR DEFENSES UNDETECTED

There is a rapid increase in network traffic encryption, with a large percentage of the Internet traffic currently encrypted. Due to such high rates of encryption, organizations are facing new security challenges since many security devices are not designed to decrypt and encrypt network traffic at high speeds, creating bottlenecks in the network and causing costly network outages.

Encrypted traffic can provide a blind spot for attackers to exploit. Within this blind spot, they can easily hide malicious content like malware and ransomware, delivering it to the network undetected. Attackers and malicious insiders can also cause costly data breaches by using the encrypted blind spot to smuggle data out of the network. In addition, malware

CHALLENGE

The rising volume of SSL/TLS encryption is enabling cyber attackers to encrypt attack traffic and evade traditional security solutions. As a result, organizations experience crippling data breaches and downtimes with high operational and financial implications.

SOLUTION

The A10 Thunder SSLi and OPSWAT MetaDefender ICAP Server combined solution provides comprehensive enterprise security for organizations. Thunder SSLi's high-performance SSL/TLS decryption provides complete visibility to the MetaDefender's advanced multi-scanning, data sanitization and data loss prevention solutions.

BENEFITS

- Gain full visibility into encrypted traffic to uncover hidden attacks
- Improve threat detection accuracy to almost 100% using multi-scanning
- Eliminate embedded threats with content disarm and reconstruction (CDR)
- Increase ROI by augmenting your entire security infrastructure and reducing downtime
- Deploy and manage easily with access to real-time actionable insights

OPSWAT.

authors are coming up with more complex attack techniques, hiding executable malware and Trojans in macro-enabled productivity documents created in software like Microsoft Word, etc. These files are generally ignored by traditional malware inspection or sandboxing solutions.

THE A10 NETWORKS SSL INSIGHT AND OPSWAT METADEFENDER ICAP SOLUTION

UNCOVER AND STOP HIDDEN THREATS CONCEALED IN ENCRYPTED TRAFFIC

Thunder SSLi eliminates the blind spot caused by SSL/TLS encryption, offloading SSL decryption and encryption functions from security devices while ensuring compliance with privacy standards. This solution works with all types of enterprise security products, augmenting them to ensure that a client's entire network is secured against encrypted threats, including: NGFWs, SWGs, IPS, UTMs, DLPs, ATP, network forensics and many more. When integrated with the advanced threat prevention, data loss prevention and data sanitization capabilities of OPSWAT's MetaDefender, the solution becomes a comprehensive, multifaceted defense against the ever-evolving cyber threat landscape.

The OPSWAT MetaDefender integrates with Thunder SSLi using the Internet Content Adaptation Protocol (ICAP). Once Thunder SSLi decrypts the traffic, it encapsulates the HTTP request/response in ICAP and forwards it to the MetaDefender ICAP Server for inspection. MetaDefender then applies multi-scanning inspection, which leverages over 30 anti-malware engines to perform advanced threat detection with an accuracy of almost 100%, going well beyond traditional signature-based and machine learning-based detection methods. MetaDefender also uses its CDR technology to ensure that no malware or Trojans can hide in macro-enabled productivity documents produced in software like Microsoft Word, etc.

SOLUTION COMPONENTS

The OPSWAT MetaDefender integrates with Thunder SSLi using the Internet Content Adaptation Protocol (ICAP) and is placed in a logical "secure decrypt zone," inspecting incoming traffic for malware and Trojans, while inspecting outgoing traffic to look out for data breaches for high-speed SSL/TLS visibility.

Encrypted traffic is intercepted and decrypted by Thunder SSLi, and the cleartext traffic is steered for inspection through any in-line security devices within the secure decrypt zone. A copy of the clear-text request/response is also sent to the MetaDefender over ICAP.

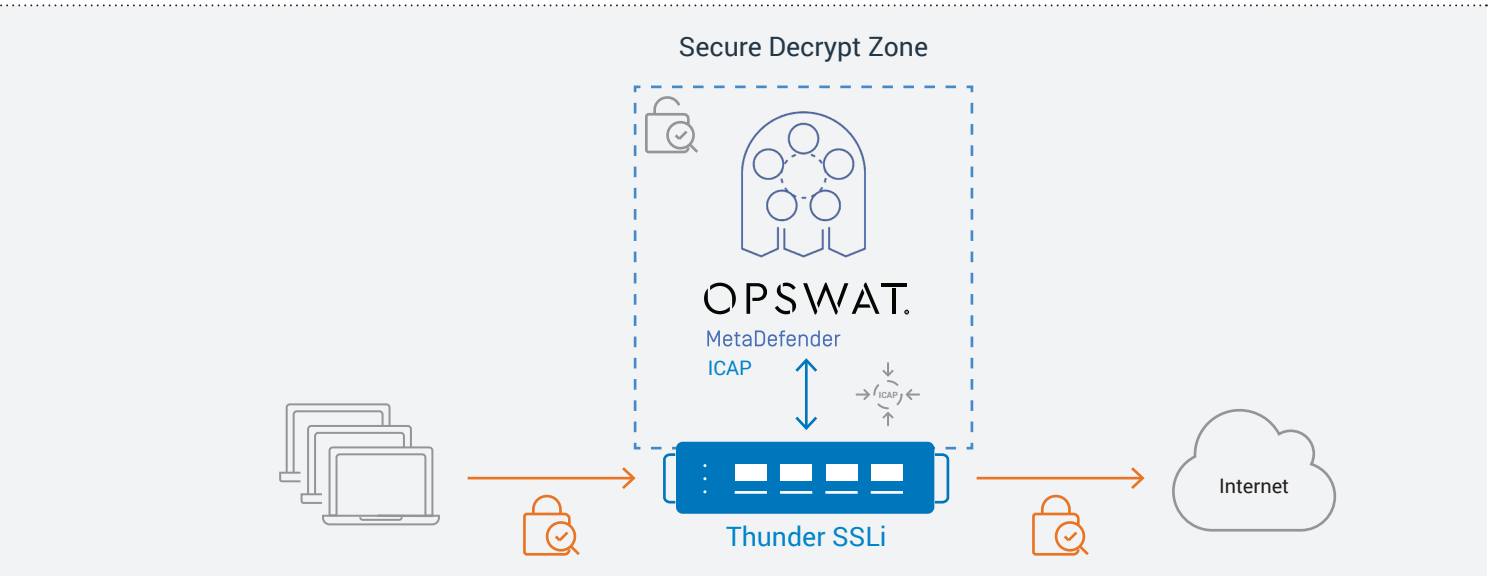

Figure 1: OPSWAT MetaDefender ICAP Server integration with Thunder SSLi

The MetaDefender ICAP Server performs advanced multi-scanning and data sanitization with CDR, making sure that no hidden malware is being delivered into the network. For outgoing traffic, the MetaDefender is on the lookout for unauthorized data extraction and makes sure sensitive assets are kept secure within the network.

FEATURES AND BENEFITS

A10 Networks SSL Insight's high-performance decryption, together with OPSWAT's MetaDefender ICAP Server enable you to:

- Gain complete visibility into network activity, including encrypted traffic, to uncover attacks and infiltrations and to deliver a safe and secure user experience
- Decrypt traffic across multiple ports and protocols for all types of network security devices
- Perform advanced threat detection and data loss prevention for complete network security
- Use multi-scanning, leveraging over 30 anti-malware engines for near 100% threat detection accuracy
- Use CDR to perform detailed malware, Trojan and virus scanning in productivity documents
- Ensure compliance with privacy standards
- Simplify deployment, operations and management
- Gain access to real-time actionable insights on network traffic, including detailed application visibility
- Reduce operational costs and increase ROI

DEFEND YOUR SENSITIVE ASSETS AGAINST ADVANCED THREATS AND DATA LOSS

With A10 Thunder SSLi's superior performance augmenting OPSWAT MetaDefender's advanced threat prevention, you can rest assured that threats, encrypted or otherwise, inbound or outbound, will be detected and blocked with high accuracy at peak performance. The ease with which this solution is deployed and managed, and the level of detailed visibility and control that this solution provides helps in strengthening your overall network security, reducing the risk of costly data breaches as well as your TCO.

NEXT STEPS

To learn more about A10 Networks' Thunder SSLi and OPSWAT's MetaDefender ICAP Server, please contact your A10 representative or visit www.a10networks.com.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

ABOUT OPSWAT

OPSWAT is a global cyber security company that has provided security solutions for enterprises since 2002. Trusted by over 1,000 organizations worldwide, OPSWAT prevents corporate damage by enabling the most effective solutions to eliminate security risks from data and devices coming into and out of an organization. For more information visit: www.opswat.com

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19199-EN-01 FEB 2019